



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/522,919

01/31/2005

Paul W Hodgson

36-1885

4217

23117

7590

03/31/2009

NIXON & VANDERHYE, PC  
901 NORTH GLEBE ROAD, 11TH FLOOR  
ARLINGTON, VA 22203

EXAMINER

TAHA, SHAQ

ART UNIT

PAPER NUMBER

2446

MAIL DATE

DELIVERY MODE

03/31/2009

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/522,919	<b>Applicant(s)</b> HODGSON, PAUL W	
	<b>Examiner</b> SHAQ TAHA	<b>Art Unit</b> 2446	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 29 December 2008.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1 - 36 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1 - 36 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 January 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

### **DETAILED ACTION**

This is a final action for application number 10/522,919 after a non-final filed on 12/29/2008. The original application was filed on 01/31/2005. Claim 1, 12, 20, 23, 30, 31, 32, and 36 are amended. Claims 1 - 36 are currently pending and have been considered below. Claims 1, 12, 20, 23, 31, 32, and 36 are independent claims.

### **Applicant's Response**

Applicant's arguments with respect to claims 1 - 36 have been considered but are moot in view of the new ground(s) of rejection.

### **Claim Rejections - 35 USC § 103**

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1 - 4, 8 - 10, 12 - 15, 22 - 24, 31 - 34 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al. (US 7,299,361), in view of Masuda et al. (US 2002/0059432) and further in view of Nielson et al. (US 6,453,327).

Regarding claims 1, 12, 23, and 36, an apparatus comprising: at least one server configured to send outgoing electronic messages on behalf of terminals connected thereto and to deliver incoming electronic messages to the terminals, each terminal

Art Unit: 2446

being accessed by one or more users, **[An incoming e-mail message is initially received at a remote e-mail server over a network, the incoming e-mail message is transmitted from the remote e-mail sever to the user computer over the network, if it is not blocked, (Kim et al., Col. 3, Lines 25-35)],**

identifying means arranged to identify the destination of the identified electronic messages, **[The e-mail message checks the identification of the NIC at the recipient end to ensure it has reached the correct destination, (Kim et al., Col. 7, Lines 27-30)],**

and processing means arranged to send a control message to each of the identified destinations, requesting suspension of delivery of the identified electronic messages, **[Once the user is notified of the infected e-mail message held by the e-mail service provider, the user may access his account and choose to delete the infected e-mail message, specify an address to which to forward the infected e-mail message, allow the infected e-mail message to remain in the quarantine server 110, or request another attempt to clean the infected e-mail message, (Kim et al., Col. 8, Lines 53-59)],**

Kim et al. fails to teach receiving traffic log data based on at least one traffic characteristics,

Masuda et al. teaches the server comprising: means arranged to generate or receive traffic log data based on at least one traffic characteristic using data derived from the handling of plural electronic messages, **[using the log data collected in the application receiving section 74 in the communication application server device**

Art Unit: 2446

**7, used amounts of the application service provided to the user can be calculated, (Masuda et al., Paragraph 310, Page 15)],**

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Kim et al. receiving traffic log data based on at least one traffic characteristics wherein using the log data collected in the application receiving section 74 in the communication application server device 7, used amounts of the application service provided to the user can be calculated, **(Masuda et al., Paragraph 310, Page 15)]**, this allows the user to select either of the network imposing higher use fees but guaranteeing the sufficient QoS or the network providing lower use fees but rendering only the best-effort type service by taking into considerations the degree of denseness in the network, use fees, characteristics of the communications applications, **(Masuda et al., Paragraph 228, Page 11)]**, to provide the service that can correspond to each of the classified classes, resources are reserved to ensure the bandwidth to be used, **(Masuda et al., Paragraph 5, Page 1),**

The modified Kim fails to teach analyzing means arranged to analyze the traffic log data as a function of a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic to identify electronic messages that satisfy the traffic characteristic criterion,

Nielsen et al. teaches each record 600 in the User's Junk E-mail database contains a "Junk E-mail Characteristics" field 601 and a "Last Date" field 603. The contents of the " Junk E-mail Characteristics " field 601 is associated with a set of text strings, **(Nielson et al., Col. 9, lines 13 – 20)**, in order to provide a mechanism for

Art Unit: 2446

identifying and automatically deleting most junk e-mail messages, **(Nielson et al., Col. 3, lines 53 – 55),**

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the modified Kim by analyzing means arranged to analyze the traffic log data as a function of a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic to identify electronic messages that satisfy the traffic characteristic criterion wherein Nielsen et al. teaches each record 600 in the User's Junk E-mail database contains a "Junk E-mail Characteristics" field 601 and a "Last Date" field 603. The contents of the " Junk E-mail Characteristics " field 601 is associated with a set of text strings, **(Nielson et al., Col. 9, lines 13 – 20),** in order to provide a mechanism for identifying and automatically deleting most junk e-mail messages, **(Nielson et al., Col. 3, lines 53 – 55).**

Regarding claims 2 and 13, an apparatus wherein said server includes: first means arranged to receive a signal identifying whether or not an identified electronic message is related to an electronic message virus, **[if a virus is detected in an e-mail message from a blocked sender, (Kim et al., Col. 6, Lines 5-7),**

and second means arranged to receive data indicative of the success or otherwise of the control message and, in the event that the received signal identifies an electronic message to be a virus and the control message is successful, to trigger deletion of the said identified electronic message, **[when an infected e-mail message cannot be cleaned. For example, one course of action may be to delete the e-mail**

Art Unit: 2446

**message or the infected portion of the e-mail message, such as the infected e-mail attachment, (Kim et al., Col. 6, Lines 32-35)].**

Regarding claims 3 and 14, an apparatus wherein: in the event that a received signal identifies an electronic message to be a virus and the control message is unsuccessful, the second means is arranged to trigger operation of identifying means and processing means running on a second server corresponding to the destination of the identified electronic message, **[a third-party quarantine server 110 for receiving infected e-mail messages 112 from the POP server 104, (Kim et al., Col. 4, Lines 31-35)].**

Regarding claim 4 and 15, an apparatus server wherein: in the event that a received signal identifies an electronic message not to be a virus and the control message is successful, the second means is arranged to permit delivery of the identified electronic message, **[if no virus is detected in the received e-mail message, the clean e-mail message is forwarded to the SMTP server at step 362, (Kim et al., Col. 10, Lines 19-22)].**

Regarding claim 8, an apparatus for delivering electronic messages, comprising a plurality of apparatus wherein at least one of the therein servers comprises: receiving means arranged to receive a request to suspend delivery of an identified electronic message, **[Another example of a user setting is a listing of sender addresses to be**

Art Unit: 2446

**blocked. Blocking a sender's address results in all e-mail messages from the blocked sender to be automatically deleted without being inspected for viruses or forwarded to the user, (Kim et al., Col. 5, Lines 53-67)],**

and wherein, in response to receipt of a said request, polling means is arranged to check delivery of the identified electronic message, and in the event that it has not been delivered, to block retrieval thereof, **[Blocking a sender's address results in all e-mail messages from the blocked sender to be automatically deleted without being inspected for viruses or forwarded to the user, (Kim et al., Col. 5, Lines 53-67)].**

Regarding claim 9, an apparatus wherein: the at least one server includes deleting means for deleting an electronic message, **[Blocking a sender's address results in all e-mail messages from the blocked sender to be automatically deleted without being inspected for viruses or forwarded to the user, (Kim et al., Col. 5, Lines 53-67)],**

and in response to receipt of a signal identifying that an identified electronic message is related to an electronic message virus, the deleting means is arranged to check whether retrieval of the identified electronic message has been blocked, and if it has, to delete it, **[when an infected e-mail message cannot be cleaned. For example, one course of action may be to delete the e-mail message or the infected portion of the e-mail message, such as the infected e-mail attachment,**



**(Kim et al., Col. 6, Lines 32-35)].**

Regarding claim 10, an apparatus wherein: in the event that the identified electronic message is related to an electronic message virus, and the identified electronic message has not been blocked, the server is arranged to invoke its identifying means and processing means in respect of electronic messages sent by the identified destinations, **[Listing the e-mail virus-detection service provider allows the recipient user to easily and more securely identify those e-mail messages sent or forwarded by the third party e-mail virus-detection service provider prior to opening of the e-mail message, (Kim et al., Col. 6, lines 22-27)].**

Regarding claim 22, Tangible computer-readable storage media containing a computer program, or a suite of computer programs, comprising a set of instructions to cause a computer, or a suite of computers, to perform the method according to claim 12, **[a network including the Internet) can be the computer readable storage medium, (Kim et al., Col. 11, Lines 14-16)].**

Regarding claim 24, a server according to claim 23, the server comprising:  
identifying means arranged to identify the destination of said identified electronic messages, **[The e-mail message checks the identification of the NIC at the recipient end to ensure it has reached the correct destination, (Kim et al., Col. 7, Lines 27-30)],**

Art Unit: 2446

and processing means arranged to send a control message to each of the identified destinations requesting suspension of delivery of the identified electronic messages, **[Once the user is notified of the infected e-mail message held by the e-mail service provider, the user may access his account and choose to delete the infected e-mail message, specify an address to which to forward the infected e-mail message, allow the infected e-mail message to remain in the quarantine server 110, or request another attempt to clean the infected e-mail message, (Kim et al., Col. 8, Lines 53-59)].**

Regarding claims 31 and 32, a tangible computer-readable storage medium having a computer program thereon for sending and receiving electronic messages, the program being executable on a terminal having a user interface, **[An incoming e-mail message is initially received at a remote e-mail server over a network, the incoming e-mail message is transmitted from the remote e-mail sever to the user computer over the network, if it is not blocked, (Kim et al., Col. 3, Lines 25-35)],**

the computer program being configured to perform the following steps when executed: (a) invite a user to input at the user interface send instructions for sending one or more electronic messages, **[forwarded to the sender or a notification e-mail message is sent to the user notifying the user that an infected e-mail message was received from the blocked sender for purposes of notifying or warning the user of potentially infected e-mail messages from a certain sender ,(Kim et al., Col. 6, Lines 7-11)],**

(b) determine if traffic log data based on handling a plurality of electronic messages meets a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic, **[The quarantine server 110 receives all e-mail messages 112 determined to be infected by the POP server 104, wherein if infected, it doesn't meet the criteria, (Kim et al., Col. 8, Lines 6-8)],**

(c) if the criterion is met, invite the user to input at the user interface a confirmation input to confirm the send instructions, **[The quarantine server 110 also includes an interface to allow cleaning, deleting, and/or sending of notification e-mail messages to the user, (Kim et al., Col. 8, Lines 10-12)],**

(d) upon receipt of the confirmation input, transmit the electronic messages from the terminal, **[forwarded to the sender or a notification e-mail message is sent to the user notifying the user that an infected e-mail message was received from the blocked sender for purposes of notifying or warning the user of potentially infected e-mail messages from a certain sender ,(Kim et al., Col. 6, Lines 7-11)],**

and (e) transmit authentication data associable with the transmitted electronic messages, **[Each user profile would typically include, for example, the username, the password required to access the user's account, the forwarding e-mail address, conditions or rules for forwarding of e-mail messages, (Kim et al., Col. 5, Lines 22-26)].**

Regarding claim 33, a terminal according to claim 31, wherein: the terminal is configured to transmit the authenticating data in encrypted form, **[PGP (pretty good**

Art Unit: 2446

**protection) encryption may be utilized to encrypt the e-mail message forwarded by the system 100, (Kim et al., Col. 7, Lines 13-15)].**

Regarding claims 34, a storage medium according to claim 31, wherein: the computer program thereon is configured, when executed, to request a user to input password data as part of the confirmation instructions, and to only permit the terminal to send authentication data once the password data has been input by the user, **[Each user profile would typically include, for example, the username, the password required to access the user's account, the forwarding e-mail address, conditions or rules for forwarding of e-mail messages, (Kim et al., Col. 5, Lines 22-26)].**

Art Unit: 2446

Claims 5 – 7 and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al. (US 7,299,361), in view of Masuda et al. (US 2002/0059432) and further in view of Toyoshima et al. (6,298,349).

Regarding claims 5 and 16, The modified Kim et al. teaches an apparatus according to claim 1, wherein said server includes including: first storage for storing details data relating to such electronic messages, **[the quarantine server 110 may hold and store the infected e-mail message for the user and to notify the user that an infected e-mail message is being held for the user, (Kim et al., Col. 8, Lines 38-42)],**

The modified Kim et al. fails to teach mapping between users and organizational units which users belong to.

further storage for storing a mapping between users and organizational units to which the users belong, the system management program 220 stores names and identifiers (employee numbers) of employees user who belong to this subordinate organization into the personnel-organization database 26, **(Toyoshima et al., Col. 7, Lines 58-62)],** display means for displaying a plurality of images, each representative of an organizational unit, **[FIG. 4 is a drawing illustrating an image displayed on the display device 200 in accordance with the group display function of the system management program 220, (Toyoshima et al., Col. 8, lines 6-10),** wherein the server is arranged, in use, such that in response to a request for data relating to a user, the first storage is arranged to output data identifying electronic messages emanating from

Art Unit: 2446

that user, **[The quarantine server 110 cleans the infected e-mail message of the viruses, if the infected e-mail message can be cleaned, and forwards the cleaned e-mail message 118 to the SMTP e-mail service server 114, (Kim et al., Col. 4, Lines 53-56)]**, the further storage is arranged to output data identifying which of the organizational units that user belongs to, **[the GUI module 222 outputs data, which is entered by a system administrator via the keyboard 204 or the like, to the database access module 224 and a given one of the GUIs 228, (Toyoshima et al., Col. 7, lines 6-11)]**, and, for those electronic messages that are identified to satisfy the criterion, the display means is arranged to insert, on the image corresponding to the identified organizational unit, a visual identifier representative of the volume or type of identified electronic messages, **[in accordance with the network system 1 of this invention, it is possible to visually display subordinate organizations of users in association with constituents of the network system 1, (Toyoshima et al., Col. 12, lines 60-65)]**, to provide a system resource display apparatus and a method for use in a network system, comprising a plurality of devices such as computers or the like connected via a network, which are arranged to display information relating to hardware and/or software resources of each of the devices in association with users and organizational groups that possess the devices, **(Toyoshima et al., Col. 1, lines 35-40)**,

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the modified Kim by mapping between users and organizational units which users belong and displaying a plurality of images, each

Art Unit: 2446

representative of an organizational unit, **(Toyoshima et al., Col. 7, Lines 58-62)**, to provide a system resource display apparatus and a method for use in a network system, comprising a plurality of devices such as computers or the like connected via a network, which are arranged to display information relating to hardware and/or software resources of each of the devices in association with users and organizational groups that possess the devices, **(Toyoshima et al., Col. 1, lines 35-40)**.

Regarding claims 6 and 17, an apparatus according to claim 5, wherein: for those electronic messages that are identified to satisfy the criterion, the display means is arranged to display a list of users on an associated image, **[FIG. 5 shows a computer system 500 that includes a display or monitor 502, screen 504, cabinet 506, keyboard 508, and mouse 510. Mouse 510 can have one or more buttons for interacting with a graphical user interface, (Kim et al., Col. 11, lines 1-5)]**,

and for each user on the list, to display details of the volume and/or type of identified electronic messages emanating therefrom, **[Kim et al., Fig. 6, Ref # 502]**.

Regarding claims 7 and 18, an apparatus according to claim 6, wherein: the display means is arranged to insert a link between the identified organizational unit and the organizational unit corresponding to the identified destination, **[However, these arrows are illustrative of any interconnection scheme serving to link the subsystems, (Kim et al., Col. 11, lines 34-37)]**.

Art Unit: 2446

Claims 11, 19, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al. (US 7,299,361), in view of Masuda et al. (US 2002/0059432) and further in view of Tarbotton et al. (6,757,830).

Regarding claims 11 and 19, The modified Kim teaches an apparatus according to claim 1, wherein: the criterion includes at least one of size of electronic message, **[The POP e-mail server 104 may impose a limit on the size of each incoming e-mail message, such as a 2 megabyte size limit, (Kim et al., Col. 7, lines 55-60)],**

The modified Kim et al. fails to teach that criteria includes an electronic message type or number of electronic messages emanating from a user,

Tarbotton et al. teaches that the criteria includes an electronic message type, **[Characteristics that may be used to determine the minimum delay period applied include sender characteristics, recipient characteristics, attachment type characteristics and message content type characteristics, (Tarbotton et al., Abstract),**

and (c) number of electronic messages emanating from a user, **[FIG. 5 illustrates characteristics of a number of example received e-mail messages and how the rules of FIG. 4 may produce a minimum delay period for each message, (Tarbotton et al., Col. 8, lines 15-18),** to detect the unwanted properties as soon as an e-mail message is received or whilst it is being stored for the minimum delay period, and then these tests repeated only if they have been updated once the minimum delay period has expired, **(Tarbotton et al., Col. 3, lines 60-65),**



It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the modified Kim by including an electronic message type, characteristics that may be used to determine the minimum delay period applied include sender characteristics, recipient characteristics, attachment type characteristics and message content type characteristics, **(Tarbotton et al., Abstract)**,

and (c) number of electronic messages emanating from a user, **(Tarbotton et al., Col. 8, lines 15-18)**, to detect the unwanted properties as soon as an e-mail message is received or whilst it is being stored for the minimum delay period, and then these tests repeated only if they have been updated once the minimum delay period has expired, **(Tarbotton et al., Col. 3, lines 60-65)**.

Regarding claims 35, Kim et al. teaches one server configured to send outgoing electronic messages on behalf of terminals connected thereto and to deliver incoming electronic messages to the terminals, each terminal being accessed by one or more users, an incoming e-mail message is initially received at a remote e-mail server over a network, the incoming e-mail message is transmitted from the remote e-mail sever to the user computer over the network, if it is not blocked, **(Kim et al., Col. 3, Lines 25-35)**,

Kim et al. fails to teach a threshold data volume originates from a common terminal or user as a criteria,

Tarbotton et al. teaches the criterion is met if traffic tog data corresponding to a target electronic message indicates that a threshold number of electronic messages

Art Unit: 2446

and/or a threshold data volume originates from a common terminal or user, in a time interval during which the target electronic message was sent, **[FIG. 5 illustrates characteristics of a number of example received e-mail messages and how the rules of FIG. 4 may produce a minimum delay period for each message, (Tarbotton et al., Col. 8, lines 15-18),** to detect the unwanted properties as soon as an e-mail message is received or whilst it is being stored for the minimum delay period, and then these tests repeated only if they have been updated once the minimum delay period has expired, **(Tarbotton et al., Col. 3, lines 60-65),**

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the modified Kim by including an electronic message type, characteristics that may be used to determine the minimum delay period applied include sender characteristics, recipient characteristics, attachment type characteristics and message content type characteristics, **(Tarbotton et al., Abstract),** and (c) number of electronic messages emanating from a user, **(Tarbotton et al., Col. 8, lines 15-18),** to detect the unwanted properties as soon as an e-mail message is received or whilst it is being stored for the minimum delay period, and then these tests repeated only if they have been updated once the minimum delay period has expired, **(Tarbotton et al., Col. 3, lines 60-65).**

Art Unit: 2446

Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al. (US 7,299,361), in view of Toyoshima et al. (6,298,349) and further in view of Nielson et al. (US 6,453,327).

Regarding claim 20, Kim et al. teaches an apparatus according to claim 1, wherein said server includes including: first storage for storing details data relating to such electronic messages, **[the quarantine server 110 may hold and store the infected e-mail message for the user and to notify the user that an infected e-mail message is being held for the user, (Kim et al., Col. 8, Lines 38-42)],**

Kim et al. fails to teach mapping between users and organizational units which users belong to.

further storage for storing a mapping between users and organizational units to which the users belong, the system management program 220 stores names and identifiers (employee numbers) of employees user who belong to this subordinate organization into the personnel-organization database 26, **(Toyoshima et al., Col. 7, Lines 58-62)],**

display means for displaying a plurality of images, each representative of an organizational unit, **[FIG. 4 is a drawing illustrating an image displayed on the display device 200 in accordance with the group display function of the system management program 220, (Toyoshima et al., Col. 8, lines 6-10),**

wherein the server is arranged, in use, such that in response to a request for data relating to a user, the first storage is arranged to output data identifying electronic

Art Unit: 2446

messages emanating from that user, **[The quarantine server 110 cleans the infected e-mail message of the viruses, if the infected e-mail message can be cleaned, and forwards the cleaned e-mail message 118 to the SMTP e-mail service server 114, (Kim et al., Col. 4, Lines 53-56)],**

the further storage is arranged to output data identifying which of the organizational units that user belongs to, **[the GUI module 222 outputs data, which is entered by a system administrator via the keyboard 204 or the like, to the database access module 224 and a given one of the GUIs 228, (Toyoshima et al., Col. 7, lines 6-11)],**

and, for those electronic messages that are identified to satisfy the criterion, the display means is arranged to insert, on the image corresponding to the identified organizational unit, a visual identifier representative of the volume or type of identified electronic messages, **[in accordance with the network system 1 of this invention, it is possible to visually display subordinate organizations of users in association with constituents of the network system 1, (Toyoshima et al., Col. 12, lines 60-65)],** to provide a system resource display apparatus and a method for use in a network system, comprising a plurality of devices such as computers or the like connected via a network, which are arranged to display information relating to hardware and/or software resources of each of the devices in association with users and organizational groups that possess the devices, **(Toyoshima et al., Col. 1, lines 35-40),**

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Kim by mapping between users and organizational units

Art Unit: 2446

which users belong and displaying a plurality of images, each representative of an organizational unit, **(Toyoshima et al., Col. 7, Lines 58-62)**, to provide a system resource display apparatus and a method for use in a network system, comprising a plurality of devices such as computers or the like connected via a network, which are arranged to display information relating to hardware and/or software resources of each of the devices in association with users and organizational groups that possess the devices, **(Toyoshima et al., Col. 1, lines 35-40)**,

The modified Kim fails to teach analyzing means arranged to analyze the traffic log data as a function of a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic to identify electronic messages that satisfy the traffic characteristic criterion,

Nielsen et al. teaches each record 600 in the User's Junk E-mail database contains a "Junk E-mail Characteristics" field 601 and a "Last Date" field 603. The contents of the " Junk E-mail Characteristics " field 601 is associated with a set of text strings, **(Nielson et al., Col. 9, lines 13 – 20)**, in order to provide a mechanism for identifying and automatically deleting most junk e-mail messages, **(Nielson et al., Col. 3, lines 53 – 55)**,

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the modified Kim by analyzing means arranged to analyze the traffic log data as a function of a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic to identify electronic messages that satisfy the traffic characteristic criterion wherein Nielsen et al. teaches

Art Unit: 2446

each record 600 in the User's Junk E-mail database contains a "Junk E-mail Characteristics" field 601 and a "Last Date" field 603. The contents of the " Junk E-mail Characteristics " field 601 is associated with a set of text strings, **(Nielson et al., Col. 9, lines 13 – 20)**, in order to provide a mechanism for identifying and automatically deleting most junk e-mail messages, **(Nielson et al., Col. 3, lines 53 – 55)**.

Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al. (US 7,299,361), in view of Toyoshima et al. (6,298,349) and further in view of Tarbotton et al. (6,757,830).

Regarding claim 21, The modified Kim teaches an apparatus wherein: the criterion includes at least one of size of electronic message, **[The POP e-mail server 104 may impose a limit on the size of each incoming e-mail message, such as a 2 megabyte size limit, (Kim et al., Col. 7, lines 55-60)],**

The modified Kim et al. fails to teach that criteria includes an electronic message type or number of electronic messages emanating from a user,

Tarbotton et al. teaches that the criteria includes an electronic message type, **[Characteristics that may be used to determine the minimum delay period applied include sender characteristics, recipient characteristics, attachment type characteristics and message content type characteristics, (Tarbotton et al., Abstract),**

and (c) number of electronic messages emanating from a user, **[FIG. 5 illustrates characteristics of a number of example received e-mail messages and how the rules of FIG. 4 may produce a minimum delay period for each message, (Tarbotton et al., Col. 8, lines 15-18),** to detect the unwanted properties as soon as an e-mail message is received or whilst it is being stored for the minimum delay period, and then these tests repeated only if they have been updated once the minimum delay period has expired, **(Tarbotton et al., Col. 3, lines 60-65),**

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the modified Kim by including an electronic message type, characteristics that may be used to determine the minimum delay period applied include sender characteristics, recipient characteristics, attachment type characteristics and message content type characteristics, **(Tarbotton et al., Abstract),**

and (c) number of electronic messages emanating from a user, **(Tarbotton et al., Col. 8, lines 15-18),** to detect the unwanted properties as soon as an e-mail message is received or whilst it is being stored for the minimum delay period, and then these tests repeated only if they have been updated once the minimum delay period has expired, **(Tarbotton et al., Col. 3, lines 60-65).**

Art Unit: 2446

Claims 25 – 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al. (US 7,299,361), in view of Masuda et al. (US 2002/0059432) and further in view of Khanna et al. (US 2002/0133604).

Regarding claim 25, The modified Kim et al. teaches a server according to claim 1, the server being arranged to receive authentication data from a terminal connected thereto, the authentication data being associated with one or more electronic messages, **[Each user profile would typically include, for example, the username, the password required to access the user's account, the forwarding e-mail address, conditions or rules for forwarding of e-mail messages, (Kim et al., Col. 5, Lines 22-26)],**

and the processing means being arranged to execute a decision to send a suspension request to the identified destination of that message in dependence on the comparison made by the comparison stage, **[Once the user is notified of the infected e-mail message held by the e-mail service provider, the user may access his account and choose to delete the infected e-mail message, specify an address to which to forward the infected e-mail message, allow the infected e-mail message to remain in the quarantine server 110, or request another attempt to clean the infected e-mail message, (Kim et al., Col. 8, Lines 53-59)],**

The modified Kim fails to teach that the server having configured to make a comparison between traffic log data corresponding to an identified message and the authentication data corresponding to-that message,



Khanna et al. teaches the login unit to incorporate the authentication data in the at least one user entry that corresponds to the at least one instruction set in the instruction set database, wherein the login unit is to store log data related to logging in the user into the web site, **(Khanna et al., Claim 10, Page 8)**, to retrieve the log data from the server, **(Khanna et al., Claim 10, Page 8)**,

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the modified Kim by including that the server is configured to make a comparison between traffic log data corresponding to an identified message and the authentication data corresponding to-that message, the login unit to incorporate the authentication data in the at least one user entry that corresponds to the at least one instruction set in the instruction set database, wherein the login unit is to store log data related to logging in the user into the web site, **(Khanna et al., Claim 10, Page 8)**, to retrieve the log data from the server, **(Khanna et al., Claim 10, Page 8)**.

Regarding claim 26, a server according to claim 25, wherein: the authentication data is received in encrypted form, **[PGP (pretty good protection) encryption may be utilized to encrypt the e-mail message forwarded by the system 100, (Kim et al., Col. 7, Lines 13-15)]**,

the comparison stage being configured to decrypt the encrypted authentication data and to compare the decrypted data with the traffic log data, **[The other key is a private key that the user uses to decrypt the messages the user receives, (Kim et**

Art Unit: 2446

al., Col. 7, Lines 2—22)].

Regarding claim 27 and 30, a terminal for sending and receiving electronic messages to and from a server according to claim 25, wherein the terminal has an interface, the interface having: a user input for receiving send instructions to send one or more specified electronic messages to a server, **[An incoming e-mail message is initially received at a remote e-mail server over a network, the incoming e-mail message is transmitted from the remote e-mail sever to the user computer over the network, if it is not blocked, (Kim et al., Col. 3, Lines 25-35)],**

the user input being configured to receive a confirmation input from the user to confirm the send instructions, **[forwarded to the sender or a notification e-mail message is sent to the user notifying the user that an infected e-mail message was received from the blocked sender for purposes of notifying or warning the user of potentially infected e-mail messages from a certain sender ,(Kim et al., Col. 6, Lines 7-11)],**

and wherein: in response to the confirmation input, the terminal is configured to send the specified electronic messages towards the server and to send authentication data associable with the specified electronic messages, **[Each user profile would typically include, for example, the username, the password required to access the user's account, the forwarding e-mail address, conditions or rules for forwarding of e-mail messages, (Kim et al., Col. 5, Lines 22-26)].**

Regarding claim 28, a terminal according to claim 27 wherein: the terminal is configured to detect whether a traffic characteristic criterion relating to the specified electronic message is met, **[The quarantine server 110 receives all e-mail messages 112 determined to be infected by the POP server 104, wherein if infected, it doesn't meet the criteria, (Kim et al., Col. 8, Lines 6-8)],**

and to request a confirmation input from a user at the user interface in response to the criterion being met, **[The quarantine server 110 also includes an interface to allow cleaning, deleting, and/or sending of notification e-mail messages to the user, (Kim et al., Col. 8, Lines 10-12)].**

Regarding claim 29, a terminal according to claim 27, wherein: the terminal is configured to transmit the authenticating data in encrypted form, **[PGP (pretty good protection) encryption may be utilized to encrypt the e-mail message forwarded by the system 100, (Kim et al., Col. 7, Lines 13-15)].**

### **Conclusion**

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Shaq Taha** whose telephone number is 571-270-1921. The examiner can normally be reached on 8:30am-5pm Mon-Fri.

Art Unit: 2446

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Jeff Pwu** can be reached on 571-272-6798.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free?).

/S. T./

Examiner, Art Unit 2446

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2446